RTX

Top 10
Cyber Best Practices

May 2024

Disclaimer: References and tools are provided for education and awareness purposes only and does not constitute an endorsement by RTX and RTX Business Units.

In partnership with leaders from across RTX Corporation (RTX) and the Defense Industrial Base (DIB) community, we have created this Top 10 Cyber Best Practices guidebook. This resource highlights steps your company can take today to reduce risk and provides awareness on available resources to promote resiliency.

These best practices are applicable to any industry and are a starting point on steps you can take to help reduce risk. Each section briefly describes the best practice, phased actions to take, and available resources and services. This list is not inclusive of all resources and services available.

For questions – please contact ecs@rtx.com and supplier_cybersecurity@rtx.com

Top 10 Cyber Best Practices

- Enable Multi-Factor Authentication
- Conduct Patching
- Perimeter Hardening
- Administrative Rights
- Install and Update Anti-virus/Malware
- Eliminate Default Passwords
- Utilize DNS Mitigations
- Conduct Email Filtering
- Web Content Filtering
- Provide Training & Awareness

Actions your company can take today to reduce risk

Disclaimer: References and tools are provided for education and awareness purposes only and does not constitute an endorsement by RTX and RTX Business Units.

Multi-Factor Authentication (MFA)

MFA is vital for your company's network security as it adds an extra layer of authentication, ensuring that even if passwords are compromised, unauthorized access is thwarted. It mitigates the risks of phishing, brute force attacks, and enhances overall protection, crucial in today's digital landscape where cyber threats are prevalent. Implementing MFA fortifies your company's network, safeguarding sensitive data and user accounts effectively.

Steps to better security:

1. Require MFA for remote network-level access (VPN)
2. Require MFA for remote access to internal tools (WebVPN)
3. Require MFA for elevated privileges
4. Implement MFA on all accounts

Resources:

- **MFA Guidance | RTX | Open To: DIB**
  - **Summary:** Shares guidance from RTX for MFA implementation.
  - **Information:** MFA Guidance document

- **Project Spectrum | DoD OSBP | Open To: DIB**
  - **Summary:** Provides small businesses with cybersecurity information, resources, tools, and training via a comprehensive and cost-effective platform.
  - **Information:** https://www.projectspectrum.io

Patching

Vulnerability management and patching are crucial for your company's network security as they help identify and fix software vulnerabilities before hackers can exploit them. Regular patching ensures that your systems are up-to-date with the latest security enhancements, protecting against known exploits and potential breaches. Proactive management of vulnerabilities minimizes the risk of cyberattacks, strengthens your company's network defenses, and safeguards sensitive data and operations.

Steps to better security:

1. Update operating systems and applications on end user systems, even while they are remote
2. Update operating systems and applications on any system that is exposed to the Internet.

Disclaimer: References and tools are provided for education and awareness purposes only and does not constitute an endorsement by RTX and RTX Business Units.

3. Establish vulnerability management program to identify and remediate new vulnerabilities.

Resources:

- **Vulnerability Scanning | NSA | Open To: DIB**
    - **Summary:** Leverages commercial scanning services to conduct asset discovery and vulnerability assessment scans of a DIB company's internet-facing networks; vulnerabilities are prioritized based on NSA's knowledge of targeting.
    - **Information:** Cybersecurity Collaboration Center (nsa.gov)

Perimeter Hardening

Perimeter hardening is crucial for your company's network as it strengthens outer defenses, making it harder for unauthorized users and malicious entities to breach your company's system(s). By implementing firewalls, intrusion detection systems, and access controls, it creates a robust first line of defense, reducing the risk of cyberattacks and unauthorized access. Proper perimeter security helps to ensure that only legitimate traffic enters your company's network, enhancing overall safety and data protection.

Steps to better security:

1. Apply "deny any/any" statements at all network firewalls.

2. Block inbound and outbound remote access protocols for all hosts (e.g., SMB, NetBIOS, WINS, RDP).

3. Only allow DNS, NTP from centrally managed infrastructure (e.g., DNS Forwarders).

4. Capture netflow, firewall, and DNS logs for traffic to and from the internet.

Resources:

- **DCISE^{3} – Dark Cubed | DC3/DCISE | Open To: CDC's**
    - **Summary:** Compares DIB company firewall logs against DIB, USG, and commercial threat feeds. Enables proactive tipping to DIB companies on vulnerabilities, compromises, and malicious scanning activity.
    - **Information:** https://www.dc3.mil/About-DC3/Capabilities-and-Services/

- **Vulnerability Disclosure Program (VDP) | DC3/DCISE | Open To: CDC's**
    - **Summary:** Identifies and helps mitigate cyber-based vulnerabilities by sharing vulnerability data with DIB companies.
    - **Information:** https://www.dc3.mil/Missions/Vulnerability-Disclosure/Vulnerability-Disclosure-Program-VDP/

Administrative Rights

Controlling administrative rights is vital for your network security because it limits the number of users who can make significant changes, reducing the risk of accidental misconfigurations or intentional malicious activities. By restricting these privileges, your company can minimize the potential impact of security breaches and prevent unauthorized access to critical systems and sensitive data. This proactive approach can enhance overall network stability, safeguard against internal threats, and maintain the integrity of your company's IT infrastructure.

Steps to better security:

1. Create separate accounts for administrative rights; do not allow users to routinely run with elevated privileges.

2. Establish a clear policy for how elevated privileges can be used (e.g., install approved software from trusted location, minor configuration changes to endpoints, administration of servers, etc.).

3. Make use of escalated privileges auditable.

Resources:

- **Microsoft Best Practices | Microsoft | Open To: Open Source**
    - **Summary:** Identifies best practices on security configurations, security identifiers and employment of least privilege principle.
    - **Information:** Microsoft – Implementing Least-Privileged Administrative Models , Microsoft - Security Identifiers , Microsoft - Interactive Login: Machine Inactivity Limit

- **Microsoft – Configure CMMC Level 2 Identification and Authentication (IA) controls | Microsoft | Open To: All**
    - **Summary:** Provides guidance for the Identification and Authorization (IA) domain. There's a table with links to content that provides step-by-step guidance to accomplish the practice.
    - **Information:** https://learn.microsoft.com/en-us/azure/active-directory/standards/configure-cmmc-level-2-identification-and-authentication

Anti-virus/Malware

Malicious code protection is essential for your company's network because it prevents harmful software like viruses and malware from infiltrating your company's systems. It safeguards sensitive data, maintains system integrity, and ensures uninterrupted operations by blocking malicious attacks that could compromise network's security and

Disclaimer: References and tools are provided for education and awareness purposes only and does not constitute an endorsement by RTX and RTX Business Units.

functionality. Regular updates and robust protection mechanisms are vital to thwart evolving cyber threats.

Steps to better security:

1. Establish an enterprise standard for AV i.e. Windows, OSX, Linux.
2. Deploy AV across fleet and establish processes to monitor health on:
    a. installed externally connected hosts (i.e., internet-facing accessible devices).
    b. installed on all capable devices.
3. Collect and analyze AV logs.

Resources:

- **DCISE[3] – Dark Cubed | DC3/DCISE | Open To: CDC's**
    - **Summary:** Compares DIB company firewall logs to DIB, USG, and commercial threat feeds. Enables proactive tipping to DIB Partners on vulnerabilities, compromises, and malicious scanning activity.
    - **Information:** https://www.dc3.mil/About-DC3/Capabilities-and-Services/

- **Vulnerability Scanning | NSA | Open To: DIB**
    - **Summary:** Leverages commercial scanning services to conduct asset discovery and conduct vulnerability assessment scans of DIB company's internet-facing networks; vulnerabilities are prioritized based on NSA's knowledge of targeting.
    - **Information:** Cybersecurity Collaboration Center (nsa.gov)

- **DoD – Cyber Awareness Challenge 2022 | DoD | Open To: DIB**
    - **Summary:** Provides guidance on malicious code and how to protect a company's information systems from it.
    - **Information:** https://dl.dod.cyber.mil/wp-content/uploads/trn/online/disa_cac_2022_final_web/pdf/DISA_CAC2022_MaliciousCode.pdf

Default Passwords

Changing default passwords is critical for your company's network security as default passwords are often widely known and exploited by attackers. By using unique and strong passwords for devices and systems, your company can significantly reduce the risk of unauthorized access and potential breaches. It's a fundamental security practice that forms a crucial barrier against common, easily preventable threats.

Steps to better security:

1. Change default credentials on all devices that are not centrally managed (e.g., printers, scanners, cameras, networking equipment, IoT devices).
2. Use unique passwords for each device.
3. Integrate into identity management, when able to.

Resources:

- **CISA Password Guidance | CISA | Open To: DIB**
    - **Summary:** Identifies risks of default passwords on the internet
    - **Information:** https://www.cisa.gov/news-events/alerts/2013/06/24/risks-default-passwords-internet

- **CIRT Default Password Database| CIRT | Open To: DIB**
    - **Summary:** Consolidates of default passwords for commercial software and hardware products.
    - **Information:** https://cirt.net/passwords

DNS Mitigations

Hardening DNS is essential for network security as it prevents DNS-related attacks, like cache poisoning and domain hijacking. Implementing secure configurations and using techniques like DNSSEC (DNS Security Extensions), helps ensure the integrity of domain resolution, reducing the risk of users being redirected to malicious websites. Hardened DNS enhances overall network trustworthiness, safeguarding against various cyber threats and ensuring users access legitimate and safe online resources.

Steps to better security:

1. Establish a DNS service that is authoritative for internal domains and a forwarder for external domains and enforce its use for corporate hosts.
2. Consider the use of commercial services that categorize domain names and provide category level controls.
3. Capture and analyze DNS traffic.
4. Implement DNSSEC for primary domains.

Resources:

- **Protective Domain Name System (PDNS) | NSA | Open To: DIB**
    - **Summary:** Combines commercial cyber threat feeds with NSA intelligence to review external DNS queries and block known or suspected malicious resolutions.

- **Information:** https://www.nsa.gov/About/Cybersecurity-Collaboration-Center/PDNS/

Email Filtering

Email filtering is crucial for your company's network as it blocks phishing attempts, malware, and spam before they reach users' inboxes, reducing the risk of malicious attacks. By accurately identifying and isolating suspicious emails, filtering systems prevent employees from falling victim to scams and clicking on harmful links, helping to ensure data security and user safety. Robust email filtering enhances overall network reliability and protects sensitive information, helping to maintain a secure communication environment.

Steps to better security:

1. Ensure all business emails are passing through email security stack (i.e., do not use domains with MX records that point to anything other than your company's email gateway).
2. Monitor email attachments for viruses.
3. Configure TLS, SPF, DKIM, and DMARC to preventing spoofing and ensure confidentiality.

Resources:

- **Spam Filtering Methods | Web Tech Experts| Open To: All**
  - **Summary:** Provides an overview of spam-fighting techniques.
  - **Information:** https://josephmuciraexclusives.com/spam-filtering-methods/

- **Best Spam Filter for Business | Titan HQ™ | Open To: All**
  - **Summary**: Shares different types of spam filters and the deployment options available.
  - **Information:** https://www.spamtitan.com/best-spam-filter-for-business/

Web Content Filtering

Filtering web content is vital for your company's network as it prevents access to malicious websites, reducing the risk of malware infections and phishing attacks. It can also help conserve bandwidth by restricting access to non-essential websites, optimizing network performance for essential business operations.

Steps to better security:

1. Require end users to use web proxy to browse the internet.

Disclaimer: References and tools are provided for education and awareness purposes only and does not constitute an endorsement by RTX and RTX Business Units.

2. Collect and analyze proxy logs.

3. Develop policies to tailor user interaction with categories of sites (e.g., pornography, gambling, hacking, etc.).

Resources:

- **Web Content Filtering and Protections | DHS | Open To: DIB**
  - **Summary:** Provides protection at the application layer for web traffic by blocking access to suspicious websites, preventing malware from running on systems and networks, and detecting and blocking phishing attempts as well as malicious web content.
  - **Information:** https://www.dhs.gov/sites/default/files/publications/privacy-pia-nppd-einstein3a-may2016.pdf

- **Simply Intuitive Cybersecurity | DC3/DCISE | Open To: CDC's**
  - **Summary:** Identifies and helps mitigate cyber-based vulnerabilities by sharing vulnerability data with DIB companies.
  - **Information:** Department of Defense Cyber Crime Center (DC3) > About DC3

Training & Awareness

Security training and awareness are vital for your network as they educate users about cyber threats, safe practices, and how to recognize phishing attempts, reducing the risk of human error-based breaches. Well informed employees are a first line of defense, capable of identifying and reporting suspicious activities, strengthening your company's overall security posture. Regular training and awareness programs foster a security-conscious culture, ensuring everyone contributes to maintaining a secure environment, safeguarding sensitive data and systems.

Steps to better security:

1. Training on phishing emails, device management/care, internet connectivity, password best practices, and reporting potential threats and reporting incidents; include phishing exercises that provide on-demand training for failures.

2. Training on BEC (Business Email Compromise), QR Codes (embedded in emails), and other social engineering campaigns.

3. Training the company's Help Desk on targeted Help Desk phishing.

4. Train users on use of escalated privileges.

Resources:

- **National Cybersecurity Alliance | NCA | Open To: All**

Disclaimer: References and tools are provided for education and awareness purposes only and does not constitute an endorsement by RTX and RTX Business Units.

    - **Summary:** Provides resources for online safety basics and recommendations for businesses to protect data and devices to create a more secure, interconnected world.
    - **Information:** https://staysafeonline.org/resources/online-safety-basics/, https://staysafeonline.org/cybersecurity-for-business/protect-data-and-devices/

- **Blue Cyber Initiative | DAF | Open To: DIB**
    - **Summary:** Provides consultations, cybersecurity webinars, and refers DAF small businesses to state/fed resources, and collaborates across federal, academic, and national small business ecosystem.
    - **Information:** https://www.safcn.af.mil/CISO/Small-Business-Cybersecurity-Information/

- **Project Spectrum | DoD OSBP | Open To: DIB**
    - **Summary:** Provides small businesses with cybersecurity information, resources, tools, and training via a comprehensive and cost-effective platform.
    - **Information:** https://www.projectspectrum.io

- **Cyber Assist | ND-ISAC | Open To: DIB**
    - **Summary:** Provides trusted resources to assist DIB companies and suppliers of varying sizes with the implementation of cyber protections, and awareness of cyber risk, regulations, and accountability for their supply chain.
    - **Information:** https://ndisac.org/dibscc/cyberassist/

Disclaimer: References and tools are provided for education and awareness purposes only and does not constitute an endorsement by RTX and RTX Business Units.

Acronyms

- AV – Anti-Virus
- BEC – Business Email Compromise
- CCC – Cyber Collaboration Center
- CDC – Cleared Defense Contractor
- DC3 – DoD Cyber Crime Center
- DCISE – DoD-Defense Industrial Base Collaborative Information Sharing Environment
- DISA – Defense Information Systems Agency
- DIB – Defense Industrial Base
- DKIM – DomainKeys Identified Mail
- DMARC – Domain-based Message Authentication, Reporting & Conformance
- DNS – Domain Name Service
- DoD – Department of Defense
- IoT – Internet of Things
- MX – Mail Exchange
- NSA – National Security Agency
- NTP – Network Time Protocol
- OSBP – Office of Small Business Programs
- RDP – Remote Desktop Protocol
- SCC – Sector Coordinating Council
- SMB – Server Message Block
- SPF – Sender Policy Framework
- TLS – Transport Layer Security
- USG – United States Government
- VPN – Virtual Private Network
- WINS – Windows Internet Name Service